Cyberdefence 24

28.09.2016

JOHN MATHERLY DLA CYBERDEFENCE24: SHODAN POZOWOLI NA SKUTECZNIEJSZĄ WALKĘ Z BOTNETAMI

O przeglądarce Shodan, niebezpieczeństwach związanych z nią oraz jej przyszłości mówi w wywiadzie dla Cyberdefence24.pl mówi John Matherly.

Cyberdefence24: Czym tak naprawdę jest Shodan?

Shodan jest rodzajem wyszukiwarki, która przeszukuje globalną sieć, w poszukiwaniu urządzeń do niej podłączonych. Zbieramy informacje o urządzeniach podłączonych do sieci, są to kamery internetowe, lodówki, czy urządzenia do kontroli elektrowni atomowych. Jeżeli taka sieć, czy urządzenie jest podpięte do internetu, to sprawdzamy gdzie jest zlokalizowane, jakiego używa oprogramowania oraz jaką posiada specyfikację techniczną. Po zebraniu tych wszystkich informacji tworzymy bazę danych dostępną dla naszych użytkowników czy klientów firmowych.

Cyberdefence24: Co tak naprawdę odróżnia Shodan od innych wyszukiwarek internetowych jak Google?

Google przeszukuje World Wide Web (WWW) i sprawdza strony pod kątem zawartości na nich. Shodan z kolei indeksuje jedynie urządzenia, na których postawione są np. strony. Nie przeszukujemy jedynie stron czy samego www, ale wszystkie urządzenia podłączone do sieci. Shodan tak jak podkreślałem nie ściąga żadnych danych, tak jak to jest w przypadku serwera pocztowego. Nie pobieramy żadnych danych ani wiadomości. Co więcej skanujemy także urządzenia wykorzystywane do przesyłania wiadomości i wszystko to co jest poza samą usługą internetową jaką jest WWW. Jedyne informacje jakie przechowujemy to metadane o samych urządzeniach.

Cyberdefence24: Dlaczego postanowiłeś stworzyć Shodan?

Od co najmniej 20 lat istnieje takie narzędzie jak NetCraft. Celem tej firmy jest tworzenie ankiet i statystyk dotyczących centrów danych i tego z jakich usług internetowych one korzystają. Firma prowadzi porównania, statystki oraz przewiduje pewne zachowania w globalnej sieci jeżeli chodzi o wykorzystanie technik komunikacji. Mogą pokazać np. wzrost aktywności w Next Generation Network (NGN). Proste zobrazowanie, jakie wersje są obecnie używane, jak wygląda ich rozkład w sieci i tego typu informacje. Pomyślałem, że mogę stworzyć coś podobnego jak NetCraft, jednak z większą ilością danych na temat samych urządzeń.

Do tego chciałem stworzyć wyszukiwarkę, która nie będzie skupiać się tylko na jednej usłudze sieciowej, ale na całym internecie. Tak aby firmy mogły korzystać z wiedzy na temat własnej sieci, czy osób, które korzystają z ich sieci. Również czy oprogramowanie w routerach jest odpowiednio często aktualizowane, jak wygląda połączenie zdalne z siecią. Chciałem stworzyć coś, czego nie sprawdzał

NetCraft, czyli wszystkiego co nie jest stroną internetową. Myślałem, że Shodan może być narzędziem do informowania firm teleinformatycznych.

Chodzi o takie przedsiębiorstwa jak Cisco, które chciałby by sprawdzać, kto używa naszych maszyn i gdzie one obecnie się znajdują. Ale również informacje o rozwiązaniach wykorzystywanych przez konkurencje. W tym przypadku chodziło lepszych i tańszych rozwiązań firmom. Nie zaprojektowałem Shodana początkowo jako narzędzie wykorzystywanego przez firmy cyberbezpieczeństwa, czy producentów sprawdzających bezpieczeństwo swoich urządzeń. Początkowo, myślałem, że moja wyszukiwarka, będzie po prostu pokazywać firmom, jak ich rozwiązania są wykorzystywane.

Cyberdefence24: Czy każdy może swobodnie korzystać z Shodana?

Mamy różne poziomy dostępu do samej wyszukiwarki i danych jakie później są wyświetlane na ekranie komputera. Każdy ma możliwość wyszukiwania podstawowych informacji w sieci, nie pobieramy za to żadnych opłat. Jednak pobieramy opłaty za ilość wyników, każdy darmowy użytkownik, może przejrzeć jedynie kilka z nich. Mój pomysł w tym miejscu polegał na tym, że zwykły użytkownik może jedynie zobaczyć kilka przykładowych wyników. Tak więc można przy darmowej sprawdzić, ile obecnie podłączonych do sieci jest tzw. Smart TV. Jednak jeżeli ktoś chce uzyskać adresy IP tych urządzeń, to musi za nie po prostu zapłacić.

Cyberdefence24: Czy za dostęp do wyników można płacić w Bitcoinach?

Nie.

Cyberdefence24: Czy Shodan może pomagać w wyszukiwaniu sieci Botnet, wykrywaniu urządzeń takich jak Internet Rzeczy?

To już się dzieje, obecnie można w Shodan wyszukać serwery Command and Control, które zarządzają sieciami botnet. Jednak nie korzystamy z tradycyjnych metod, jakie są obecnie wykorzystywane przez firmy cyberbezpieczeństwa. Stosują one inżynierie wsteczną wobec wirusów, potem lokalizują serwer na bazie kodu, który udało się odczytać w wirusie. Oczywiście taki sposób na wykrywanie sieci botnet działa, jednak jest czasochłonny i wymaga zarażenia jakiegoś urządzenia, bez próbki wirusa nie ma możliwości jego zbadania. Nasze podejście jest kompletnie inne. Możemy na swoim sprzęcie udawać, że zostaliśmy zarażeni i dzięki temu odkryć centra kontroli zanim zaczną prowadzić kampanie rozsiewające wirusy. Współpracujemy także z firmami w tym sektorze działania Shodan.

Jeżeli chodzi o ransomware, tu sprawa nie wygląda tak prosto. Wszystko zależy od osób, które prowadzą samą kampanię. Początkowo większość połączeń ransomware była przekierowywana przez sieć Tor. Część z nich możemy wykryć, jeżeli osoby odpowiedzialne za kampanie źle skonfigurują porty, tak że dane ich kampanie wyciekają do publicznej sieci. Jednak w przypadku innych kampanii, jest to zdecydowanie trudniejsze zadanie. Nie zamierzamy także w najbliższej przyszłości stać się wyszukiwarką w ukrytej sieci Tor. Inne firmy aktualnie tym się zajmują. Podejrzewam, że niedługo cały ruch, jeżeli chodzi o kampanie ransomware zniknie. Ofiary zmądrzeją i zaczną stosować jeszcze lepsze zabezpieczenia niż do tej pory.

Cyberdefence24: Czy zamierzacie skanować deepweb albo darknet?

Nie zamierzamy. Robimy kilka rzeczy w tym kierunku, jednak nie jest to obecnie usługa oferowana na naszej stronie. Jeżeli zaczęlibyśmy przeszukiwać deepweb, to trudniej było by dopasować wyszukiwarkę dla osób, które korzystają za darmo z Shodan. Nie tylko chodzi o koszty związane z samą dodatkową infrastrukturą, chodzi także o zawartość tej sieci, która w większości jest nielegalna. Jeżeli zaczęlibyśmy pobierać dane z tych serwerów, które zawierają te nielegalne treści to bardzo trudno byłoby to przekazać naszym użytkownikom. Nasza polityka nie tylko polega na przygotowaniu

odpowiedniego narzędzia dla naszych komercyjnych klientów, ale także dla wszystkich użytkowników.

Jednak robimy niektóre rzeczy w tym obszarze, np. jesteśmy wstanie zidentyfikować węzły Tor, przez które przepływa większość ruchu w tej sieci. Jednak nie skanujemy ich obecnie tak, aby dane o nich były dostępne publicznie.

Cyberdefence24: Powiedziałeś podczas dzisiejszej konferencji, że nie ma czegoś takiego jak anonimowe przeglądanie sieci. Dlaczego jednak tak trudno, agencjom czy firmom wskazać, palce kto jest odpowiedzialny za niektóre ataki?

Atrybucja jest bardzo trudna do stwierdzenia, pokazanie kto tak naprawdę odpowiada za atak jest czasami nie do określenia. Przykład, ustawiłem własne honeypoty, tak aby wykrywały kto skanuje całą sieć, dokładnie - Industrial Control System (ICS). Udało mi się znaleźć kogoś, kto używał bardzo mało znanego protokołu, niewiele osób nawet szuka informacji pod tym adresem. Analizując przepływ informacji okazało się, że głównym źródłem ruchu jest serwer w Holandii. Dopiero po dłuższym skanowaniu okazało się, że tak naprawdę ruch generowała grupa badawcza z uniwersytetu w Chinach. Wynajmowali oni serwer w Holandii. Byli bardzo otwarci jeżeli chodzi o swoje badania, pokazywali co robią, jednak nie wspomnieli, że wykorzystują serwery poza granicami. To pokazuje, jak trudno dokonać atrybucji ruchu sieciowego, czy źródła ruchu sieciowego. Jednocześnie wykrywanie samych działań jest bardzo proste.

Cyberdefence24: Czy sztuczna inteligencja może pomóc w skanowaniu sieci, może pomóc ukrywać ślady przestępcom?

Jeżeli spojrzymy na sztuczną inteligencję, to pomoże ona w klasyfikowaniu informacji, identyfikacji urządzeń. Obecnie jeżeli skanujmy w poszukiwaniu złośliwego oprogramowania, szukamy sygnatur. Cała branża jest na tym skupiona, ale moim zdaniem sygnatury są po prostu głupie. Sztuczna inteligencja może być inną drogą, aby przestać wyszukiwać sygnatur, a skupić się na bardziej dopasowanych i mądrzejszych rozwiązaniach. Chodzi o odczytywanie tajnych informacji przekazywanych przez sieć. Z mojej perspektywy sztuczna inteligencja pomoże bardzo mocno w klasyfikowaniu samego ruchu i urządzeń sieciowych.

Cyberdefence24: Skanujecie przy pomocy Shodan, centra danych oraz centra danych wykorzystywanych przy tworzeniu chmury obliczeniowej?

Chmura jest jeszcze gorzej zabezpieczona niż sama sieć. Zdecydowanie łatwiej tam coś znaleźć.

Dobrym przykładem tutaj jest MongoDB. Przez działania i wyszukiwania Shodan, MongoDB pojawiało się wielokrotnie w wiadomościach i na portalach informacyjnych. Większość serwerów MongoDB jest postawiona na chmurze obliczeniowej firmy Amazon. Niebezpieczne są tutaj obrazki wykorzystywane przez użytkowników. Możesz spokojnie wpisać w adres przeglądarki stronę Amazon, przejść do działu Digital Ocean i poprosić o zbudowanie bazy MongoDB. I wszystko dzieje się jak za dotknięciem czarodziejskiej różdżki. Cały dział rozwoju usunął panel administracyjny. Teraz osoby odpowiedzialne za rozwój swoich stron nie mają dostępu do ustawień bezpieczeństwa swojej bazy.

Chmura obliczeniowa posiada dużo więcej niezabezpieczonych urządzeń i hakerzy są w pełni świadomi takiej sytuacji. Jeżeli wstawisz cokolwiek do chmury, to zauważysz zwiększoną ilość ataków na swoja infrastrukturę. Ponieważ, żeby zdobyć adres, hakerzy nie muszą skanować wszystkich adresów IP, skanują jedynie serwery dostępne w sieci. Bardzo łatwo stać się celem ataków w sieci.

Cyberdefence24: Czy przy pomocy Shodana da się zlokalizować elektrownie nuklearną podłączoną do sieci? Czy zdarzyło ci się kiedykolwiek, aby osoby o złych zamiarach wykorzystały Shodan do odnalezienia lokalizacji infrastruktury krytycznej?

Jest to dosyć popularne pytanie. Pytanie zwykle dotyczy tego samego, czy ułatwiasz pracę ludziom o złych zamiarach. Odpowiedź na to jest dosyć prosta z mojej strony, proceder ten miał miejsce jeszcze zanim powstał sam Shodan. Cyberprzestępcy używali botnetów do skanowania sieci i szukania luk w systemach. Warto to wspomnieć statystykę dotyczącą Windowsa XP. Chodziło dokładnie o podłączenie do sieci, brzmiało to tak – Jeżeli używasz Windows XP, to w ciągu 15 min twoja maszyna zostanie zagrożona atakiem – To było jeszcze zanim powstał Shodan. Nigdy jednak nie udawaliśmy, że coś takiego może mieć miejsce, jednak każdy kto używa Shodan nie jest anonimowy. Nie pozwalamy na używanie Bitcoinów, nie akceptujemy anonimowych sposobów płatności. Posiadamy odpowiednie praktyki, aby każdy kto używa naszej wyszukiwarki nie był anonimowy. Od samego początku pokazywaliśmy, że jeżeli wykorzystasz Shodan do czegoś nielegalnego, to nie będziesz przez naszą firmę w żaden sposób chroniony.

Jeżeli chodzi o systemy kontroli jakie znajdują się choćby w elektrowniach atomowych. Jest bardzo duża różnica pomiędzy możliwością wyszukania samego systemu podłączonego do sieci, a możliwością jego wykorzystania. Szczególnie jeżeli chodzi o duże systemy przemysłowe, są one specjalnie zaprojektowane do swoich zadań. Zostały przystosowane do lokalizacji w której znajduje się sieć, inżynierowe także w pewnym stopniu wprowadzają własną konfigurację w systemach, podczas swojej pracy. W dodatku system dostosowany jest do procesów, którymi zarządza.

Jeżeli teraz odpalisz Shodan, to nie będziesz wstanie odnaleźć elektrowni atomowej. Musisz posiadać wiedzę inżyniera nuklearnego, żeby wiedzieć czego szukać. To nie Google, gdzie można po prostu wpisać frazę *elektrownia atomowa* i naszym oczom ukaże się system elektrowni atomowej. Shodan tak nie działa. Żeby wykorzystać Shodan w pełni, musisz posiadać bardzo specyficzną i wysoką technicznie wiedzę, żeby odnaleźć dokładnie to czego szukasz. W dodatku, jeżeli będziesz wstanie się do nich podłączyć, to nie oznacza, że będziesz mógł spowodować wybuch. Jest to bardzo trudne do wykonania.

Cyberdefence24: Jeżeli jednak użytkownikowi uda się znaleźć elementy infrastruktury krytycznej to nie uważasz, że osoby odpowiedzialne za bezpieczeństwo tej infrastruktury, robią coś nie tak?

Właśnie dlatego przesyłamy wszystkie swoje znaleziska do CERT-ów za darmo. Nie pobieramy za to żadnych opłat. I oni reagują zwykle na to natychmiastowo, w przypadku elektrowni atomowych, jest czasami nawet kwestia kilkunastu sekund, zanim odłączą system od globalnej sieci.

Cyberdefence24: Czy macie kontakt z przedstawicielami infrastruktury przemysłowej, podczas swojej codziennej pracy?

Nie, nie mamy. Zwykle wszystkie sprawy właśnie załatwiamy przez stworzone do tego CERTy. Po pierwsze dlatego, że po prostu zwykle nie wiedzą czym jest Shodan. Czasami kontaktujemy się z organem zarządzającym samą infrastrukturą. Wysyłamy np. odpowiednie informacje do polskiego CERTu, potem oni kontaktują się z osobami odpowiedzialnymi za infrastrukturę. Ponieważ, jeżeli my skontaktujemy się z samą firmą, to kontakt będzie znikomy. Zapytają jedynie dlaczego kontaktujemy się z nimi w tej sprawie, co się dzieje. Jednak jeżeli podmiotem, który się będzie z nim kontaktował będzie Polski rząd to sprawę potraktują poważnie i zabezpieczą swoje systemy bardzo szybko.

Cyberdefence24: Jakie masz plany na przyszłość?

Więcej skanowania i więcej danych. Chcemy wykrywać więcej połączeń sieciowych, szczególnie tych niezabezpieczonych. Kolejnym wyzwaniem pozostaje dla nas Internet Rzeczy. Warto wspomnieć to co prezentował Mikko Hypponen podczas swojej prezentacji, o czajniku podłączonym do sieci. Na Shodan nie ma ich wiele, może jeden, maksymalnie dwa. Jednak pojawiają się. Chcemy dodać więcej

funkcjonalności do samej wyszukiwarki oraz skupić się na większym zakresie zbierania metadanych. Posłużę się tu przykładem nowych telewizorów Samsunga. Te urządzenia mają w swoich systemach serwery webowe. Dzięki temu można uzyskać informacje o numerze modelu, rozdzielczości jakiej używa, informacji z jakiej sieci WiFi korzysta. Zaczynamy dodawać więcej warstw metadanych, które zbieramy o samych urządzeniach podłączonych do sieci. Chcemy robić to samo co do tej pory, jednak po prostu więcej i zagłębiając się mocniej w samą tematykę sieci.

John Matherly jest kartografem internetowym, mówcą oraz założycielem Shodan, pierwszej na świecie wyszukiwarki wszystkich urządzeń łączących się z internetem.

Czytaj też: Wyciekły dane z globalnego spisu przestępców